A synopsis on

On the irreducibility of certain polynomials

Submitted to

Swami Ramanand Teerth Marathwada University
Nanded-431606, Maharashtra, India

For the Degree of

Doctor of Philosophy(Ph.D.)

In Mathematics
(Faculty of Sciences and Technology)

Submitted by

Syed Zarqua mohammedi
Research Student

Under the Guidance of

Dr Usha K Sangale
Assistant Professor
School of Mathematical Sciences
SRTM University, Nanded-431606.

August 2023

On the irreducibility of certain polynomials

Ms Syed Zarqua mohammedi

1 Abstract

Given a polynomial with integer coefficients, whether this polynomial is irreducible over rationals or not is an important question. If it is reducible, then what can we say about the degree of its irreducible factors in terms of the coefficients is another problem of interest. The classical irreducibility criteria by Eisenstein was rephrased by Dumas in the language of Newton polygons. In recent years, the concept of Newton polygon has seen a lot of applications to determine the irreducibility of polynomials, to find the Galois group associated with these irreducible polynomials. We wish to pursue such problems in our research and hope to though new light in this direction.

2 Introduction

A polynomial is said to be reducible over a given field if it is expressible as a product of lower degree polynomials with coefficients in this field. Otherwise it is irreducible polynomial.
In other words, A polynomial $f(x) \in \mathbb{Z}[x]$ is irreducible (or irreducible over $\mathbb{Z}$) provided that $f(x) \not\equiv \pm 1$ and whenever $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Z}[x]$, either $g(x) \equiv \pm 1$ or $h(x) \equiv \pm 1$. If $f(x) \in \mathbb{Z}[x]$ is not irreducible and is not $0, 1, -1$, then $f(x)$ is reducible. It is customary to treat the polynomials $0, 1, -1$ as neither reducible nor irreducible.

We are interested in the question of deciding whether a given polynomial is irreducible or not. As a consequence we use some tests to check whether given polynomial is reducible or not. For example, the well known Gauss' Lemma says that *let* $f(x) \in \mathbb{Z}[x]$ *with* $\deg f(x) \geq 1$. *If* $f(x)$ *is irreducible over* $\mathbb{Z}$, $f(x)$ *is irreducible over* $\mathbb{Q}$. Furthermore, if $f(x)$ is irreducible over $\mathbb{Q}$ and gcd of its coefficient is 1, then $f(x)$is irreducible over $\mathbb{Z}$.

There is an important connection between irreduciblity of polynomials over $\mathbb{Z}$ and irreducibility over $\mathbb{Q}$. Eisenstein's criteria states that *let* $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ *where* n *is a positive integer. Suppose that there exist a prime* p *such that* $p \nmid a_n, p | a_j$*for all* $0 \leq j < n$ *and* $p^2 \nmid a_0$.*Then* $f(x)$ *is irreducible over* $\mathbb{Q}$. But unfortunately no such criterion is devised which is applicable for all polynomials. However, a number of tests for irreducibility criteria have been found so far which give valuable information for some particular classes of polynomials. Kronecker has given a general solution of the problem of completely factoring or decomposing

a rational integral polynomial into the product of irreducible polynomials in a finite number of steps. Perron gives irreducibility criteria as follows *If* $f(x) = \sum_{j=0}^{n} a_j x^j \in Z[x]$ *with* $n \geq 1$ *is such that* $a_n = 1, a_0 \neq 0$, *and* $|a_{n-1}| > 1 + |a_{n-2}| + |a_{n-3}| + \ldots |a_0|$, *then* $f(x)$ *is irreducible.* Dumas used the notion of Newton polygon and studied the Irreducibility of polynomials.

3 Review of Literature and Development in The Subject

The n^{th} cyclotomic polynomial denoted by $\phi_n(x)$ is the product of the monic irreducible factors of $x^n - 1$ which are not factor of $x^k - 1$ for $k \in \{1, 2, \ldots n-1\}$. Gauss stated that $\phi_n(x)$ *is irreducible for all positive integers* n.

It is an easy observation that if $f(x)$ is reducible in $\mathbb{Z}[X]$, then it is reducible over $F_p[X]$, where F_p is the finite field of p elements. Hence, we have the following criterion:

If $f(X)$ *is irreducible over* $F_p[X]$ *for some prime number* p, *then* $f(X)$*is irreducible over* $\mathbb{Q}$.

Converse is not true. That is, if $f(X)$ is irreducible over $\mathbb{Q}$, then it is not necessarily irreducible over F_p for some prime number p. In [9], the authors counted the irreducible polynomials over a finite field with prescribed coefficient and set up a general combinatorial framework using generating functions with coefficients from a group algebra which is generated by equivalence classes of polynomials with prescribed coefficients. In [10], for a fixed irreducible polynomial F, the authors considered the set of all valuations on bounded by valuations whose support is (F). The first main result presents a characterization for valuations in terms of their graded rings, which is stated as follows;

Let (K, V_0) *be a valued field and* Γ_0 *its group of values. Fix a totally ordered divisible group* Γ *containing* Γ_0*and* $R = K[x]$. *Let* $V = V_0 \bigcup \{v : R \to \Gamma_\infty\}$. *Consider the partial order on* V *given by*$V_0 \leq V$ *for every* $v \in V$ *and for* $v, \mu \in V/\{v_o\}$, *we set* $v \leq \mu$ *if and only if* $v(f) \leq \mu(f)$ *for every* $f \in K[x]$.

In 1906, G. Dumas, [6] developed the notion of Newton polygon and proved many results on the irreducibility of polynomials. This criteria generalizes Eisenstein criteria.

More recently, the earlier Irreducibility criterion are put on a strong footing as a general result by Sudhesh Khanduja and their school ([2], [1]).

4 Aim and Objective of Research

The irreducibility of truncated exponential function, Bessel function, Binomial expansion etc are well known. We shall study the existing literature. We shall ask new questions and try to solve them. We expect that our finding will not only add to the literature, it will also open up new vistas for others to work on.

5 Methodology to be Adopted

Most of our research is theoretical in nature so we shall refer books and research papers of various authors and researchers who are working in this area. With the guidance of my research supervisor I will clear my doubts and difficulties. I would like to attend seminars, conferences, and any research activity related to my field of interest.

6 Importance of Study

Irreducible polynomials over finite fields are the fundamental objects in the theory of finite fields, since they are needed to construct finite fields and work with them . Their interest in theoretical aspects often appears in number theory, combinatorics and algebraic geometry, while in practical applications they are widely used in coding theory, cryptography, complexity theory, and computer science. The theory of finite fields was built in the works of Fermat, Euler, Legendre, Gauss, Galois, Dixon, and other outstanding scientists and until the last quarter of the 20^{th} century developed as a field of pure mathematics, but due to the needs of coding and cryptography, the applied aspect of the theory are now devoted to the effective implementation of Arithmetic in finite fields. The theory of polynomials of degree n in one variable, irreducible over finite field F_p^n, and for numerous applications in the modern theory of Information transfer. Irreducible polynomials whose roots form the basis for representing elements of finite fields are analogous to primes.

7 Proposed Work Plan

First Year. We shall undertake a serious study of algebraic number theory. We shall follow the book [11], [8].

Second Year. We shall learn advanced techniques in number theory. We shall follow the lecture notes of M. Filaseta to understand various irreducibility criteria.

Third Year. We shall study the research papers of M. Filaseta, T. N. Shorey, S. K. Khanduja, Anuj Jakhar.

Fourth Year. We shall figure out new problems, which may be a further generalizations of the existing results, new questions arising on the way of our study and understanding.

Fifth Year. We shall write down our finding and send them for publication in peer reviewed journals.

References

[1] Anuj Zakhar. (2020). On the factors of a polynomial. Bull LMS. 52, 158-160

[2] Khanduja, S. K., and Saha, J. (1997). On a generalization of Eisenstein's irreducibility criterion. Mathematika, 44(1), 37-41.

[3] Abdymanapov, S., Turusbekova, U., Turginbayeva, A., and Altynbek, S. (2020). Research of irreducible normal polynomials special type over a field of characteristic 2. IAENG International Journal of Applied Mathematics, 50(4), 777-782.

[4] Cherchem, A., Bouguebrine, S., and Boughambouz, H. (2022). On the construction of irreducible and primitive polynomials from Fqm [x] to Fq [x]. Finite Fields and Their Applications, 78, 101971.

[5] Dorwart, H. L. (1935). Irreducibility of polynomials. The American Mathematical Monthly, 42(6), 369-381.

[6] G. Dumas. (1906). Sur quelques cas d'irréductibilité des polynömes à coefficients rationnels. Journal de Math. Pure et Appl., 2, 191 - 258.

[7] Girstmair, K. (2005). On an irreducibility criterion of M. Ram Murty. The American Mathematical Monthly, 112(3), 269.

[8] Sudesh K Khanduja. (2023). A textbook of Algebraic Number Theory, Springer.

[9] Gao, Z., Kuttner, S., Wang, Q. (2022). Counting irreducible polynomials with prescribed coefficients over a finite field. Finite Fields and Their Applications, 80, 102023.

[10] dos Santos Barnabé, M., Novacoski, J. (2022). Valuations on K [x] approaching a fixed irreducible polynomial. Journal of Algebra, 592, 100-117.

[11] Saban Alaca and Kenneth Williams, *Introductory algebraic number Theory*, Cambridge University Press (2003).

Ms. Syed Zarqua Mohammedi
Research Student

Dr. Usha K. Sangale
Research Guide